The Information Domain as an Element of National Power

by Robert Kozloski

Strategic Insights is a quarterly electronic journal produced by the Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

Introduction

For the past several decades, doctrine within the Department of Defense (DoD) has articulated that Diplomacy, Information, Military, and Economics (DIME) are the four sources of national power. In this article, I will demonstrate that the information component of this DIME model is not being effectively used by the United States and we are falling behind our potential adversaries when using the information domain for national security.

The Information Domain

During the cold war era, the *information* aspect of the DIME concept was more focused on strategic communications and propaganda rather than the full information spectrum. However because of the advances in technology, the information domain has become a new environment in which nations, groups and individuals can operate and advance national security objectives—similar to land, sea or air.

Basic communication models in the past included sender, receiver, transmission medium and message as separate and distinct components. Due to the significant advances in information technology, the information domain combines the previous four elements and is enabled by a variety of mediums to include the internet, radio waves, satellite communications, wireless networks, etc. The combination of these elements has formed the information domain[1] .

One example of how people are taking advantage of the information domain is the rise in popularity of the Massively Multiplayer Online Role Playing Games, such Everquest and Second Life. In this new environment people can perform day to day tasks in a parallel, virtual world. In these virtual worlds, elections are held, property is traded, and battles are fought. These virtual worlds often spill over into reality as people use actual currency to purchase new virtual characters, weapons, homes, property and status.

Militaries around the world use the same concepts to create Live, Virtual and Constructive simulation[2] networks. For example, a pilot could fly an F/A-18 simulator in North Carolina and drop a simulated bomb controlled by an Airmen in a simulator in Nevada. They both could be looking at simulated targets on the battlefield in Iraq. To take this example one step further, instead of dropping a simulated bomb, the pilot could have released a different type of weapon system such as a laser, high power electronic jamming signal or computer virus to disrupt a financial network—an entire battle could be conducted in the information domain and the results would appear in the physical domain.

A few years from now it may be possible that one could walk outside one's home in Washington, DC, look up and see sunshine, blue skies and birds flying. You would be oblivious to the fact that an unmanned air craft flying at 40,000 feet is sending electronic jamming signals to prevent a propaganda message from a terrorist cell from appearing on television sets in the region. In effect, a battle could be waged in the information domain and it may or may not appear in the physical domain.

Falling Behind

Because of the dominance of the U.S. Military's hard power compared to any near-competitor's conventional military forces, potential adversaries have developed strategies to use the information domain to project soft power to counter. In particular, potential adversaries such as China and Russia, have developed new techniques such as cyber attacks, information theft, and manipulation of the media to strike the United States in a critically vulnerable area. The United States' computer networks and space assets are its "soft ribs and strategic weaknesses."[3]

In 2000, the Russian Federation's National Security Blueprint, kontseptsiya, recognized the importance of the information domain to their national security. "There is an increased threat to the national security of the Russian Federation in the information sphere. A serious danger arises from the desire of a number of countries to dominate the global information domain space and to expel Russia from the external and internal information market; from the development by a number of states of 'information warfare' concepts that entail creation of ways of exerting a dangerous effect on other countries' information systems, of disrupting information and telecommunications systems and data storage systems, and of gaining unauthorized access to them. The level and scope of the military threat are growing."[4]

Since publishing this document, it is believed the Russian Federation has used the information domain as an instrument of their national power. During a period of increased national tension between Russia and Estonia in April 2007, Estonia's government computer systems came under a coordinated Denial of Service attack. The computer attacks inundated Estonia's Web sites, overwhelming servers and forcing them to shut down, sometimes for a few hours, sometimes longer. Mr. Mikko, the Estonian Defense Ministry spokesman, said sites that typically received 1,000 visits a day had been buried under as many as 2,000 a second.[5]

A year later, when tensions escalated with Georgia, the Russian Federation reportedly conducted a similar but more extensive attack. This attack included a similar denial of service attack directed at Georgian government websites but also included the use of propaganda, defacing websites—including replacing a picture of Georgia's President Mikhail Saakashvili with a picture of Adolph Hitler—and psychological operations. The result of this attack was to relocate the hosting of some of the Government websites to servers in Atlanta, Georgia, USA.[6]

Like Russia, China has also been linked to several computer attacks. From 2004 to 2007, two major computer attacks on U.S. Government computers, codenamed Titan Rain and Byzantine Foothold[7] , were traced back to China—not hackers operating in China but the Chinese Government. According to Col Gary McAlum, Chief of Staff for the U.S. Strategic Command's Global Network Operations Center, "China currently has the intent and capability to conduct cyber operations anywhere in the world at any time." [8]

However, China has already demonstrated its ability to go beyond cyber attacks. Private IT security experts discovered that electronic picture frames purchased at stores throughout the United States were also used to exploit computer systems. These picture frames need to be connected to a computer to download digital pictures. Embedded in the memory of the picture frame was a virus that would disable security systems and send valuable information such as

passwords back to China.[9] It is impossible to determine the amount of electronic components that handle government data that could be at risk to such exploitation.

In January 2007, the Chinese Military demonstrated it ability to shoot down a low orbiting satellite as part of its Anti-Satellite Missile program.[10] Many military experts feel that this was not only a demonstration of a weapons system but an insight to the Chinese strategy to disable Global Positioning Systems (GPS).[11]

In addition to Russia and China, Iran, Syria and Libya all have programs within their military organizations designed to execute attacks in the information domain. Terrorist groups such as Hezbollah and Al' Qaeda have also developed cyber warfare cells to support their operations.

Since the September 11, 2001 attacks terrorist groups such as Al' Qaeda have used information mediums, such as the internet, radio and television, Al Jazeera in particular, to pass operational information, recruit operators and influence public opinion throughout the world. Early in Operation IRAQI FREEDOM, the insurgents in Iraq realized the importance of manipulating public opinion. They used video to record beheadings, improvised explosive device attacks, and kidnappings and released the videos over a variety of networks. This demonstrated that the insurgents could be successful against Coalition Forces in order to illicit support from sympathizers.

The U.S. military was slow to counter this tactic and relied on the reporters from the embedded media to report its success. During the first few months of the war, when it was widely supported by the American public, the media reported the effectiveness of combat operations. Once support waned it appeared that media's focus was on body counts and the number attacks on U.S. Forces, widely ignoring military successes. As I observed during my participation in Operation IRAQI FREEDOM, that unlike the insurgents, the military did not have an effective means to report to the world what was working and the success it was having.

The Military Model

In the most recent version of the *National Security Strategy*, the Department of Defense noted that it was organizing to meet new challenges by adapting its forces to deter threats in the physical and information domains.[12] The DoD has created several different agencies to counter the new challenges and most fall under U.S. Strategic Command. The DoD also developed new doctrine which provides the frame work for U.S. military forces to operate in the information domain.

In 2006, the United States Joint Forces Command published Joint Publication 3-13, *Information Operations*. This publication defines the operational doctrine for use by all U.S. military forces. There are five main components of the Information Operations (IO) model: Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception, and Operations Security.[13]

Electronic Warfare is the use of the electro magnetic spectrum and direct energy to attack an adversary.[14] This capability could be used to destroy or disrupt an adversary's ability to communicate information. Systems and individuals that rely on wireless communications, such at cell phones, are particularly susceptible to this type of attack. Computer Network Operations are broken down into three functions: computer network defense, computer network attack, and computer network exploitation.[15] Psychological Operations are planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals.[16] Military Deception is described as those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and

operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces' mission.[17] Operations security is a process of identifying critical information and subsequently analyzing friendly actions and other activities to: identify what friendly information is necessary for the adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remain secure.[18]

These five components have been in existence for some time, however it wasn't until recently that the information domain was recognized as a viable operational environment and synergies could be gained if these five components were used together to achieve unity of effort and more effective results. This same methodology needs to be incorporated into a comprehensive strategy for the totality of the United States Government.

While the concept of Information Operations may seem unremarkable for military tactics, it is not without controversy. During Operation IRAQI FREEDOM, the Information Operations Task Force used a contracted firm to write pro-American news stories and have them printed in local papers as a means to influence the general populace. This practice was called "covert propaganda" by the Government Accountability Office and was highly criticized in an article by the *Los Angles Times*.[19]

Information Centric Organizations

In October of 2001, Secretary of Defense Rumsfeld created the Office of Strategic Influence. While little information is known about this Office's mission, it was labeled as the new propaganda arm of the Department of Defense by its critics. The Office was terminated in February of 2002 because the intense criticism no longer left it capable of completing its new mission.[20]

President Bush issued Executive Order 13283 in January 2003 establishing the Office of Global Communications (OGC). This Office assumed a strategic communications advisory role for the President and heads of departments. They also created deployable communications teams that could work to support national security in conjunction with the State and Defense Departments. The OGC coordination efforts focus on daily messages, communications planning, and long-term strategy.[21]

The State Department created the Counterterrorism Communications Center (CTCC) to coordinate strategic communications in the war of ideas. In her April 2008 testimony before the House Armed Services Committee, Secretary of State Rice described the CTCC as "Operating under the auspices of my Under Secretary of State for Public Diplomacy and Public Affairs, the CTCC is staffed by communications professionals in public affairs, public diplomacy, and psychological operations, from State, DoD, and the intelligence community, to insure synchronized communications efforts."[22]

While each of these organizations have merit, there needs to be a coordinated effort across the U.S. Government to organize in a manner that encompasses the full spectrum of the information domain.

Current Policy Shortfalls

Under the current administration several policy documents have been developed relating to the information domain.

In February 2003 the White House published the *National Strategy to Secure Cyberspace*.[23] In this document the importance of cyberspace was acknowledged for individuals, private businesses and government entities. It also stated that the use of cyberspace was vital for national and homeland security.[24] Strategic guidance was provided for the implementation of measures to protect cyberspace.

In December 2003, the President released *Homeland Security Presidential Directive—7 Critical Infrastructure Identification, Prioritization, and Protection*. In this directive the Department of Homeland Security was designated as the overall coordinator to protect critical infrastructure and key resources from terrorist attacks.[25]

In response to this directive, in 2006 the *Department of Homeland Security published the National Infrastructure Protection Plan* (NIPP). This plan sponsored by DHS and was agreed to by all executive department secretaries. The NIPP again reiterated the importance of cyberspace to national security and designated the Department of Homeland Security as the focal point for cyberspace security.[26]

The *National Strategy for Information Sharing* was released in October 2007. This document was developed in response to the recommendations outlined in the 9/11 Commission. This strategy provides strategic guidance for the sharing of information across the federal, state and local governments and with the private sector. This strategy is also closely linked with other strategies: *National Security Strategy, Homeland Security Strategy, National Strategy for Combating Terrorism,* and the *National Intelligence Strategy*.[27]

These policy elements all stress the importance of cyberspace and information to national security but none effectively address how to use the information domain as instrument of power for national security. The current policies also fail to achieve unity of effort among all federal agencies that have a roll or contribution to managing the information domain. Those missing from these polices include: Department of State, Department of Commerce (National Institute of Standards and Technology), Federal Communications Commission, and National Aeronautics and Space Administration.

Information Domain and the National Security Strategy

When the next administration rewrites the National Security Strategy it needs to outline its vision of how the use of the information domain plays a critical role in our national security. I assert there are four components that need to be addressed:

Defending the Information Domain

As previously discussed there are measures in place that provides a strategy for the protection of cyber space. These efforts need to include the full spectrum of the information domain. This must include satellite communications, television and radio systems, and wireless services.

Satellite communications provide the ability to move large amounts of information, quickly to locations throughout the world. As indicated previously our weapon and navigation systems have become dependent on GPS information systems. This data is vulnerable to an adversary's use of the electro magnetic spectrum to disrupt our transmissions. As more countries explore the use of space, the interruption or disruption of satellite information needs to be addressed.

Television and radio systems are widely used as methods for mass notification and alerting. If these systems become disabled or false information is inserted, mass panic could result. We, as a society, have become dependent on television as a source for news and information. Our

television networks could be easily taken over by an adversary and used as a tool for propaganda or misinformation.

Transmission of information over wireless devices is ubiquitous. However, they can easily be turned into monitoring devices or be used as GPS tracking tool. Another aspect of wireless transmissions that must be defended are those communications systems used by our first responders. Consider the September 11, 2001 World Trade Center attacks and the response that followed. Communications among first responders was inefficient but consider how much worse this would have been if the NYC dispatch center was shut down as a result of an adversaries' actions or if radio transmission among first responders at the incident were blocked or misinformation was injected. The jamming of first responder communications happens occasionally by U.S. citizens[28] which demonstrates its vulnerability to an organized attack.

Radio frequency scanners capable of monitoring fire department and police communications are commercially available and can be easily purchased by the general public. The information transmitted over these unsecured radio networks could be used to gain information for secondary attacks. Targeting first responders after an attack is a tactic that has been widely used by insurgents in Iraq, the Irish Republican Army and even pro-life activists after attacks on abortion clinics.[29]

Exploiting the Information Domain

The intelligence community and federal law enforcement agencies, such as the Federal Bureau of Investigations, already have systems in place to exploit the information domain. The legal issues are pretty clear when dealing with foreign adversaries however we need to develop a national strategy for exploiting the information domain on domestic threats. This would require balancing civil liberties with national security. The information domain does not recognize national boundaries and threats to national security could originate from within our national border as easily as it could come from overseas.

Protecting our Critical Information

The NIPP currently addresses methods to protect information we put into cyberspace. However the government needs to adopt a concept similar to the DoD's Operational Security Policy. We need to protect information that reveals vulnerabilities and programs that are vital for national security as well as the operations of the bureaucracy that could possibly be exploited by an adversary. Since the Johnson administration, the U.S. public trust in the Federal Government has eroded. We, as citizens, demand transparency and expect the media to hold the Government accountable to provide it. However transparency and the release of sensitive information needs to balanced with national security concerns.

As an example, defense contractors make public locations of construction of military equipment such as air craft, ships and weapon systems. While the physical security of these assets is the responsibility of the host facility, the availability of this information makes it possible for adversaries to collect information or recruit personnel for espionage. Other examples of information that should be protected: use and location of the strategic oil reserve, aging or outdated control systems, such as the nation's air traffic control systems and vulnerabilities in our economic systems. Another example of information that should be restricted is information on successful cyber attacks on government networks, such as the recent attack on the Department of Defense.[30] The release of this information to the general public lets adversaries know that their attack was successful and to the extent it disrupted operations at the targeted department. This information would be valuable for planning future attacks.

As in Instrument of Power

For decades, the information domain has been used to assert the United States' ability to create advantages and influence events[31] in the name of national security. For example, in 1942 the *Voice of America* radio service was created to get the United States strategic message out directly to the people of the world. This service is still funded today by the U.S. Government and broadcast throughout the world in over 45 languages.[32]

There are numerous examples of how the United States could use the information domain to apply its influence to global events. It could easily influence elections, support pro-American efforts, effect business transactions, create tension between nations, etc. In a recent session of the House Homeland Security Emerging Threats Subcommittee Chairman Jim Langevin, D-R.I., stated, "It [cyber warfare] is ... unchartered territory and I know the policymakers are struggling with how and when to use our offensive capabilities, it's important for the government to have a clear understanding of what our offensive capabilities are and how best to employ them and when." [33]

Conclusion

Despite entering the information age decades ago, little has changed in how the United States projects its power to support national security. The next administration must rethink the way we protect and use the information domain to this end. We must develop strategic policy and organize in manner that allows us to counter potential threats and use the information domain to our advantage.

The issue is how to effectively organize the government to best accomplish this. Unlike the other three instruments of national power, diplomacy, military and economic, there is no single department chartered to deal specifically with information. The solution must be an interagency committee that falls under the control of the National Security Council.

References

1. The DoD defines the information environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive.

2. Live – real people training in a real environment. Virtual – people using simulation devices for training, i.e. flight simulators. Constructive – virtual environments used for training, i,e. video games. These three simulation environments can be combined to achieve more realist training results.

3. US-China Economic and Security Review Commission, *USCC 2008 Annual Report*, 156.

4. Arms Control Association. "Russia's National Security Concept," Jan/Feb 2000, http://www.armscontrol.org/act/2000_01-02/docjf00.

5. Steven Lee Meyers, "Estonia Computers Blitzed, Possibly by the Russians," *New York Times*, May 19, 2007.

6. Defense Tech, "Cyber Warfare," http://www.defensetech.org/archives/cat_cyberwarfare.html.

7. "An Evolving Crisis," *Businessweek*, April 10, 2008, http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm.

8. US-China Economic and Security Review Commission, Op. Cit., 163.

9. Richard Clarke, *Your Government Failed You* (New York: Harper Collins, 2008), 315.

10. GlobalSecurity.org, "Anti-Satellite Missile Program," http://www.globalsecurity.org/space/world/china/asat.htm.

11. GPS information is widely used by navigation and weapon systems.

12. The White House, *The National Security Strategy of the United States*, March 2006, 43.

13. United States Joint Forces Command, Joint Publication-13, Information Operations, 2006, 2-1.

14. Ibid., 2-1.

15. Ibid., 2-2.

16. Ibid., 2-3.

17. Ibid., 2-4.

18. Ibid., 2-4.

19. Borozou Daragahi and Mark Mazzett, "US Military Covertly Pays to Run Stories in Iraqi Press," *Los Angeles Times*, November 30, 2005.

20. Donald Rumsfeld, "DoD News Briefing," February 26, 2002, http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=2798.

21. The Executive Office of the President, "White House Office Of Global Communications," http://www.whitehouse.gov/ogc/aboutogc.html.

22. Condoleezza Rice, "Testimony Before The House Armed Services Committee," April 15, 2008, http://armedservices.house.gov/pdfs/FC041508/RiceTestimony041508.pdf.

23. Cyberspace refers to the networking of various computer systems. Cyberspace is a component of the Information Domain.

24. *The National Strategy for Defending Cyberspace*, February 2003.

25. *Homeland Security Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.

26. *National Infrastructure Protection Plan*, 2006.

27. *National Strategy on Information Sharing*, October, 2007.

28. The National Association For Amateur Radio, "Apologetic Radio Jammer Jack Gerritsen Gets Seven Years, Fines," Sep 19, 2006, http://www.arrl.org/news/stories/2006/09/19/100/.

29. *FBI Law Enforcement Bulletin* 74, Number 5 (May 2005): 5.

30. Julian E. Barnes, "Cyber-attack on Defense Department Computers Raises Concerns," *Los Angeles Times*, November 28, 2008.

31. In April 2008 a group of experts from the DoD, congress, academia and private industry met at the National Defense University to discuss the concept of cyberpower. Dr. Dan Kuehl of NDU defines cyber power as the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power.

32. Voice of America, "About VOA," http://www.voanews.com/english/about/FastFacts.cfm.

33. Chris Strohm, "Officials Lack Policy For Taking Cyber War Offensive," CongressDaily, November 24, 2008, http://www.nationaljournal.com/congressdaily/cd_20081124_7915.php.